 <b>County of Kaua'i</b>	<b>Procedures for Protecting Personal Information</b>	<b>Documentation Number: ITP0030</b>
		<b>Revision Level: 12/31/08</b>

**I. SCOPE / PURPOSE:** The purpose of this policy is to describe the County of Kauai's (COK) procedures for protecting documents containing Personal Information.

**Background:**

The 2008 Hawai'i Session Laws Act 10 was enacted on July 8, 2008. The purpose of Act 10 is to implement recommendations of the Hawai'i Identity Theft Task Force's December 2007 report to protect the security of personal information collected and maintained by state and county government agencies.

**II. RESPONSIBILITY:** All County of Kauai agencies, boards and commission are responsible for safeguarding the confidential information with which we have been entrusted in serving the citizens of Kaua'i. Identity theft is one of the fastest-growing crimes in our state, and the proper handling of any personal information within our control is a paramount concern to the County of Kaua'i. This responsibility requires the continuing diligence of all of our employees to limit the potential for mishandling or losing personal information. Accordingly, the following procedures are to be implemented immediately and must be observed by all employees.

**III. DEFINITIONS:**

"Personal Information" is the First Name or First Initial, and Last Name, in combination with any one of the following:

- Social Security Number
- Driver's License Number or Hawai'i ID Number
- Account Number, Credit or Debit Card Number, Access Code, or Password that would permit access to an individual's financial account.


**IV. PROCEDURE:**

**A. Document Storage**

The following procedures must be observed for storing confidential documents:

1. All hardcopy confidential documents maintained by the agency shall be stored in a secured area accessible to only those employees whose job function requires them to handle such documents. A secured area includes a locked drawer, cabinet, or room. Access to these areas must be controlled and monitored.

<b>Prepared by: Nyree Norman</b>	<b>Date last revised: 12/31/08</b>	<b>Page Number: 1/6</b>
<b>Original release date: 12/24/2008</b>	<b>Reviewed by : Eric Knutzen</b>  <b>Approved by: Wallace Rezentes</b>	

 <p><b>County of Kaua'i</b></p>	<p><b>Procedures for Protecting Personal Information</b></p>	<p><b>Documentation Number: ITP0030</b></p>
		<p><b>Revision Level: 12/31/08</b></p>

2. All electronic confidential documents maintained by the agency shall be safeguarded against possible misuse by complying with the Information Technology Computer Use, USB Flash Drive, Standard Mobile Device and Document Destruction Policies as attached in Exhibit A, B, C, and D respectively.

#### B. Document Processing

Business needs frequently require that confidential documents be removed from secured areas in order to perform necessary job functions. The following procedures shall be followed when such documents are in possession of an employee in the course of the employee's job duty.


1. When not in a secured area, the confidential documents must not leave the employee's immediate control. Documents of this nature cannot be left unsupervised while physical controls are not in place.
2. When not in a secured area, precautions must be taken to obscure the confidential information from view, such as by means of an opaque file folder or envelope. Confidential information shall not be left in plain view in a vehicle.
3. Confidential documents must be inspected thoroughly to ensure they do not contain any misfiled confidential information from other files.
4. To protect electronic confidential documents, all employees shall leave their computers in a 'locked or 'logged off' state, when not in immediate vicinity of the employee's work area.
5. The County shall strive to redact personal information in electronic documents where possible, reduce any unnecessary collection of personal information, and ensure data is properly encrypted on all mobile devices.

#### C. Document Shipping

##### Shipping to an Individual or Business

Business functions frequently require that personal information be mailed to external destinations, such as Contracts, RFPs, etc. When in transit, these


<p><b>Prepared by: Nyree Norman</b></p>	<p><b>Date last revised: 12/31/08</b></p>	<p><b>Page Number: 2/6</b></p>
<p><b>Original release date: 12/24/2008</b></p>	<p><b>Reviewed by : Eric Knutzen</b>  <b>Approved by: Wallace Rezentes</b></p>	

 <p><b>County of Kaua'i</b></p>	<p><b>Procedures for Protecting Personal Information</b></p>	<p><b>Documentation Number: ITP0030</b></p>
		<p><b>Revision Level: 12/31/08</b></p>

materials are not in our immediate control and must be secured to the best of our ability beforehand. The following procedures must be observed when shipping confidential documents:

1. Preparation of Documents
  - a. Documents must be packaged in such a way as to not have any personal information viewable.
  - b. All destination addresses must be inspected thoroughly and confirmed to avoid delivery to a wrong address or person.
  - c. Ensure that the correct return address is provided in the event the package is undeliverable.
  - d. Contents of shipments must be verified to contain only appropriate information for the intended recipient.
2. Shipping Materials
  - a. Use shipping envelopes made of fibrous or polymeric material or reinforced shipping boxes made of sturdy corrugated material with a limited number of seams.
  - b. Ensure the container is the appropriate size to accommodate the secure and safe delivery of contents.
  - c. Storage containers, including certain archive boxes, are not considered suitable for shipping as they are collapsible and damage easily when navigating large distribution center equipment and processes.
  - d. Never reuse shipping containers that are worn or have been torn. Use super strength, 2 inch wide packaging tape.
  - e. Secure all seams of package with tape. Run tape completely around package, not just the flap and bottom seam. Secure package further by running tape horizontally and vertically around the center of the package.
3. Package Labeling
  - a. Be sure the shipping label includes a complete recipient name, address, and, for businesses, telephone number; and, that it also includes the sender name, return address and telephone number. The telephone numbers provide a means of contact when/if for some reason the package is misrouted or damaged during the shipping process.
  - b. Make sure the entire label is securely affixed to the center front of package and it is clearly visible.
  - c. DO NOT MARK THE PACKAGE CONFIDENTIAL.

<p><b>Prepared by: Nyree Norman</b></p>	<p><b>Date last revised: 12/31/08</b></p>	<p><b>Page Number: 3/6</b></p>
<p><b>Original release date: 12/24/2008</b></p>	<p><b>Reviewed by : Eric Knutzen</b> <b>Approved by: Wallace Rezentes</b></p>	

 <p><b>County of Kaua'i</b></p>	<p><b>Procedures for Protecting Personal Information</b></p>	<p><b>Documentation Number: ITP0030</b></p>
		<p><b>Revision Level: 12/31/08</b></p>

4. Shipping Method

- a. Packages containing confidential material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

D. Shipping between Offices

All files and records being shipped between County offices or between County and external associates must employ all of the above procedures and the following:

1. Inventory of Confidential Documents

- a. Shipper is to inventory and document all records being shipped prior to shipping.
- b. The inventory record includes, at a minimum, the name and tracking number of the record(s) being shipped, the destination, the sender name and contact number, the recipient name, the date shipped and a place to record the date of when the shipment reaches its destination.
- c. An electronic copy of this inventory must be emailed to the intended recipient notifying them of the pending arrival.

2. Timely Acknowledgment


- a. Shipper is to include a copy of the inventory document in the shipping container so that the recipient can verify contents of shipment upon arrival and acknowledge to sender that all record(s) were received.
- b. If a shipment has not been acknowledged by a recipient within 24 hours, shipper will follow-up with the recipient office and/or shipping organization as appropriate.

E. Breach Notification and Incident Reporting

If documents containing confidential information are improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. An employee shall notify the Information Technology Help Desk Administrator, and an incident-report (Exhibit D as attached) form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident.

Prepared by: Nyree Norman	Date last revised: 12/31/08	Page Number: 4/6
Original release date: 12/24/2008	Reviewed by : Eric Knutzen  Approved by: Wallace Rezentes	

 <b>County of Kaua'i</b>	<b>Procedures for Protecting Personal Information</b>	<b>Documentation Number: ITP0030</b>
		<b>Revision Level: 12/31/08</b>

2. The supervisor will communicate the situation to the reception staff or those that regularly field calls from the public so that they are prepared to answer phone inquiries by individuals who have been notified of the loss or disclosure of their records.

F. Each agency, board and commission is responsible to inform the Mayor's ISPC appointee of any additional use of personal information or pertinent changes to forms.

G. The County agencies, boards and commissions are advised not to do any of the following:

1. Intentionally communicate or otherwise make available to the general public entire SS#.
2. Intentionally print or imbed entire SS# on any card required to access products or services.
3. Require entire SS# to access an Internet website, unless a password or unique personal identification # or other authentication device is also required to access the website.
4. Print entire SS# on any material that is mailed, unless the materials are employer-to-employee communications or where specifically requested by the individual.


H. Consequences

It is the responsibility of agency supervisors to ensure their staff's compliance with these procedures. Failure by the agency employees to comply with the procedures defined in this directive may result in disciplinary action.

I. Authority

**CHAPTER 487N  
SECURITY BREACH OF PERSONAL INFORMATION**

<b>Prepared by: Nyree Norman</b>	<b>Date last revised: 12/31/08</b>	<b>Page Number: 5/6</b>
<b>Original release date: 12/24/2008</b>	<b>Reviewed by : Eric Knutzen  Approved by: Wallace Rezentes</b>	

 <b>County of Kaua'i</b>	<b>Procedures for Protecting Personal Information</b>	<b>Documentation Number: ITP0030</b>
		<b>Revision Level: 12/31/08</b>

#### **V. ATTACHMENTS:**

Exhibit A - Information Technology Computer Use Policy  
 Exhibit B - USB Flash Drive Policy  
 Exhibit C - Standard Mobile Device Policy  
 Exhibit D - Document Destruction Policy  
 Exhibit E - Personal Information Security Incident Report Form

#### **VI. ANNUAL REVIEW, REPORTING, POLICY AND OVERSIGHT RESPONSIBILITY**


The Mayor's appointee to the statewide Information, Security and Privacy Council (ISPC) is responsible to conduct an annual review of this policy, as well as to have county oversight regarding the protection of personal information. The County will work with identification of collection of unnecessary information and perform an annual review regarding the potential of any unnecessary collection of personal information, as well as redaction personal information. Furthermore, an annual report is to be submitted to the County Administration as well as to the ISPC, following any timeline so published by the ISPC.

#### **VII. REFERENCES**

For a copy of this policy or any documents referred to within this policy please refer to the following Personal Information Document Library link:

<http://cok-sp-01/Personal%20Information%20Document%20Library/Forms/AllItems.aspx>

<b>Prepared by: Nyree Norman</b>	<b>Date last revised: 12/31/08</b>	<b>Page Number: 6/6</b>
<b>Original release date: 12/24/2008</b>	<b>Reviewed by : Eric Knutzen</b>  <b>Approved by: Wallace Rezentes</b>	

 <b>County of Kaua'i</b>	<b>Information Technology Team Division Computer, Email and Internet Usage Policy</b>	<b>Documentation Number: ITP0024</b>
		<b>Revision Level: December 29, 2008</b>

#### **I. SCOPE/PURPOSE:**

The scope of this policy covers the County of Kaua'i computer hardware, Internet connection and email system. The Information Technology Division is responsible for maintaining computers, providing Internet access and an email system to the computer users of the County. The purpose of this policy is to define proper use of these systems and is applicable to every user of County computers, which are for business usage only. This policy supersedes the Internet and E-mail Policy dated March 15, 2001.

#### **II. APPLICABILITY:**

The Computer, Email and Internet Usage Policy of the County of Kaua'i is applicable to all employees of the County of Kaua'i except employees in Bargaining Unit 1. Therefore, no Unit 1 employee shall utilize the County's computer system to access the Internet or email, except while on temporary assignment (TA) to a position in another bargaining unit that provides the employee with access and use of the Internet and email. If a Unit 1 employee becomes subject to this policy because of a TA to another position outside of Unit 1 and a violation of this policy occurs, discipline shall be taken in accordance with the Unit 1 contract.

#### **III. DEFINITIONS:**

Network - interconnected group of computer equipment


User - Computer user authorized to be on the County network

#### **IV. RESPONSIBILITY:**

Use of County of Kaua'i computers, networks, Internet and email is a privilege granted by management and may be revoked at any time for inappropriate conduct including, but not limited to:

- Engaging in private or personal business activities;
- Sending chain letters;
- Handling material with pornographic or sexual content;
- Misrepresenting oneself or the County of Kaua'i;
- Engaging in unlawful or malicious activities;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Religious or political causes;
- Causing congestion, disruption, disablement, alteration, or impairment of County networks or systems;
- Infringing in any way on the copyrights or trademark rights of others;

Prepared by: Eric Knutzen	Date last revised: December 29, 2008	Page Number: 1/4
Original release date: March 15, 2001	Reviewed by : Wallace Rezentes Jr Approved by: IT Steering Committee	

 <b>County of Kaua'i</b>	<b>Information Technology Team Division Computer, Email and Internet Usage Policy</b>	<b>Documentation Number: ITP0024</b>  <b>Revision Level: December 29, 2008</b>
--	---	--

- Using recreational games;
- Defeating or attempting to defeat security restrictions on County systems and applications; and/or
- Using another person's account;
- Virus creation or propagation.

#### V. PROCEDURE:

##### A. Computer Use:

The County of Kaua'i provides computers, peripheral devices, servers and networks to the extent required for daily operations. This equipment is property of the County and will be maintained and moved by the County IT Division. Users need to protect against unauthorized access to the County computers in their area. Users are not to share their passwords with anyone, and are responsible for any misuse of their authentication information.

The County provides licensed copies of software that is installed on computers. The IT Division must approve and install all software. No County owned software may be installed on non-County computers. No unauthorized software shall be installed on County computers.

Files stored on County computers must be related to the County's Mission. No mp3, mp4, wav, mpg, .jpeg, audio or video files not related to work are to be stored on County computers.


As part of the County's efforts to have a workplace free of harassment, the County prohibits the use of computers, email or the internet in ways that are disruptive, offensive to others, or harmful to morale.

##### B. Electronic Mail:

Electronic mail is provided as a communication tool for County business purposes. Email messages should be written in a clear, concise, businesslike style, as these communications represent the County. When sending email, ensure they are addressed to individuals authorized to receive the information contained in it, does not contradict County policy, and does not contain statements that could be construed as racist, sexist, insulting or otherwise offensive. Information or attachments that are considered confidential should not be sent outside the County

<b>Prepared by: Eric Knutzen</b>	<b>Date last revised: December 29, 2008</b>	<b>Page Number:</b> 2/4
<b>Original release date: March 15, 2001</b>	<b>Reviewed by : Wallace Rezentes Jr</b> <b>Approved by: IT Steering Committee</b>	



 <b>County of Kaua'i</b>	<b>Information Technology Team Division Computer, Email and Internet Usage Policy</b>	<b>Documentation Number: ITP0024</b>
		<b>Revision Level: December 29, 2008</b>

network. Data sent outside the County's secure network is not secure and may be read by others.

Computer viruses can be contained in email attachments which could replicate through the County network, pose a security risk to County data, or hinder daily operations. Do not open suspicious email attachments, or attachments from persons you do not know.

All email messages are the property of the County, are subject to periodic, unannounced inspection and may be disclosed without user permission. This includes attachments included with email.

No email shall be retained on the County systems longer than 90 days.

County mailboxes may not exceed the limit of storage space. Users are responsible for deleting or archiving email messages from their mailbox. The email system will send warnings as mailboxes approach their size limits. If mailboxes reach their limits, they will be automatically disabled. Users must contact the helpdesk to reopen the mailbox, and must immediately clean the mailbox to prevent it from being locked again.

#### **C. Internet Use:**


The County of Kaua'i permits access to the Internet to those who require it for business purposes. Department heads may request employee access to the internet via the Internet Access Request Form, attached as Exhibit A. Before access is granted, the employee and department head shall sign the County of Kaua'i Internet Access Agreement, Exhibit B, and Acknowledgement of Receipt, Exhibit C. All employees are held responsible for abiding by this and all subsequent internet policies.

Every County computer user is responsible for ensuring that the internet service will be used in an efficient, ethical and lawful manner. The Information Technology Division monitors web sites that users visit and may disclose this information without user permission. Internet usage is regulated by the rules of conduct listed above.

The internet is largely unsecure, thus leaving the County vulnerable to attacks from hackers or viruses. For this reason, only IT personnel are allowed to download software from the internet, or install any software on County computers.

<b>Prepared by: Eric Knutzen</b>	<b>Date last revised: December 29, 2008</b>	<b>Page Number: 3/4</b>
	<b>Reviewed by : Wallace Rezentes Jr</b> <b>Approved by: IT Steering Committee</b>	
<b>Original release date: March 15, 2001</b>		

EXHIBIT A

 <p>County of Kaua'i</p>	<p><b>Information Technology Team Division Computer, Email and Internet Usage Policy</b></p>	<p><b>Documentation Number: ITP0024</b></p> <hr/> <p><b>Revision Level: December 29, 2008</b></p>
---	--	---

The County purchases services that provide bandwidth, or the capacity for data transfer of an electronic communications system. Restrictions must be placed on Internet usage for security purposes and to prevent communications reaching capacity. Web filters are in place to regulate the sites that may be visited, according to the rules of conduct, and which assists in preventing over-usage of bandwidth. Any time you have the Internet open, you are using bandwidth. Streaming media such as internet radio and on-line videos are restricted, unless expressly approved for business purposes, by submitting Exhibit B to the IT Division.

**D. ACKNOWLEDGMENT OF RECEIPT:**

The Acknowledgment of Receipt is attached as Exhibit C. When a new hire joins the County, the personnel representative in the respective department will provide a copy of this policy to the new hire. The new employee will read the policy and sign the Acknowledgment of Receipt. The original signed copy is then to be filed by the department's personnel representative, who also makes a copy and forwards to the Personnel Department for inclusion in the employee's personnel files.

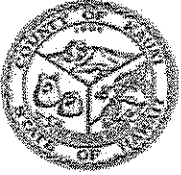
**E. ATTACHMENTS:**

Exhibit A. County of Kaua'i Add/Delete form  
Exhibit B. Internet Access Request Form  
Exhibit C. Acknowledgment of Receipt

**VI. NON-COMPLIANCE:**

Non-compliance with the County's Computer, Email and Internet policy, guidelines or procedures may result in the revocation of the Internet or email privileges and/or other appropriate disciplinary action, including reprimand, suspension and termination of employment in accordance with applicable bargaining unit agreements, or if warranted, criminal prosecution or civil liability.

Prepared by: Eric Knutzen	Date last revised: December 29, 2008	Page Number: 4/4
Original release date: March 15, 2001	Reviewed by : Wallace Rezentes Jr  Approved by: IT Steering Committee	

 County of Kaua'i (COK)	Information Technology Team Division Data Control Policy: All portable data storage, with special focus on USB Flash Drives	Documentation Number: ITP0021
		Revision Level: 1

#### I. SCOPE/PURPOSE

To clearly outline the County of Kaua'i (COK) policy regarding the use of all data storage media which can be easily moved, with special focus on USB Flash Drives.

#### II. RESPONSIBILITY:

All COK employees.

#### III. DEFINITIONS:

"Portable Data Storage" = Includes USB Flash Drives (referred to by some as memory sticks), ZIP drives, CD's as well as DVD's and any other type of data storage which data may be saved to and easily taken off COK premises.

"Easily taken off COK premises" = We are restricting this to mean that CD's, DVD's, ZIP drives, USB Flash Drives and the like may with great ease be moved off COK premises. Please use sober common sense to understand this - obviously computers can also be moved off premises but not as "easily" - as, for example, USB Flash Drives.

"USB Flash Drives" - are pocket sized ultra portable storage devices (about the size of a highlighter pen) that hold 8Mb - 5GB or more of data that can be instantly accessed from any PC with a USB port. These devices offer users a convenient alternative to floppy disks and ZIP drives, but also present a significant security challenge. Examples across the world attest to the loss of data, and resulting potential harm to others due to the ease with which large amounts of data may be brought off site or viruses, malicious software etc introduced to computers and networks.

#### IV. POLICY:


- A. No portable data storage units such as CD's, DVD's or Zip Drives may be taken off COK premises without the express permission each and every time by a Department Head.
- B. USB Flash Drives are not to be brought onto COK premises. This includes privately owned USB Flash Drives. As such, no USB Flash Drive is at any time be connected to any USB port on COK equipment, for any reason
- C. Exceptions to this are made only by the IT Steering Committee approving the purchase of USB Flash Drives by applying through the Supplemental Computer Request (SCR) application process.

#### V. REFERENCE:

This document is to be updated by the IT Manager, and is to be accessible by all County of Kaua'i employees

#### VI. ATTACHMENTS: N/A

Prepared by: Lynnette Meatoga	Date last revised: 08/25/06	Page Number: 1/1
Original release date: 08/25/06	Reviewed by : Michael Tresler  Approved by: Gary Heu, for the IT Steering Committee	

  County of Kaua'i	<b>Information Technology Team</b>  <b>Standard Mobile Device Policy</b>	Documentation Number: ITP0025
		Revision Level: October 16, 2007

#### I. SCOPE / PURPOSE:

The purpose of this document is to define the policies pertaining to all mobile devices - to ease in the efficient, effective and data secure support of such equipment. Such policies pertain to the standardization of the equipment provided, as well as the configuration and support of such mobile devices.

#### II. RESPONSIBILITY:

The Information Technology Division (IT) is responsible for supporting all mobile devices owned or leased by the County of Kaua'i. As such, the user of such mobile device is to bear the responsibility while in possession of such mobile devices to respect this policy.

User lack of respect for this policy and abuse can result the user being held accountable and can be prosecuted under applicable statutes.

#### III. DEFINITIONS:

IT an abbreviation for Information Technology

Mobile Devices: Devices including but not limited to laptops, PDA's, and smart phones.


User: Any person using mobile devices

#### IV. POLICY:

##### A. Standard mobile devices are to:

- Restricted to the use of Microsoft offered software
- Standard security software defined by the IT Division

Prepared by: Lynnette Meatoga	Date last revised: August 9, 2007	Page Number: 1/3
Original release date: August 9, 2007	Reviewed by : Eric Knutzen  Approved by: IT Steering Committee	

  County of Kaua'i	<b>Information Technology Team</b>  <b>Standard Mobile Device Policy</b>	Documentation Number: ITP0025
		Revision Level: October 16, 2007

## V. POLICY:

### A. Standard mobile devices

#### 1.1 Unacceptable use:


- Unauthorized copying of Copy-protected material (Music, Video, etc.)
- Destruction of or damage to the equipment, software or data belonging to the County of Kaua'i or other users
- Providing, assisting in or gaining unauthorized or inappropriate access to the County of Kaua'i computing resources
- Activities that interfere with the ability of others to use resources effectively (i.e., streaming radio which impacts network traffic)
- Obtain extra resources not authorized to the user, or
- Gain unauthorized access to systems by using knowledge of:
  - A special password
  - Loopholes in computer security systems;
  - Another user's password, or
  - Access abilities used during a previous position
- Harass, defame, intimidate or threaten anyone through the use of computing or network resources for sexual harassment issues
- Use computing or network resources for profit, commercial or political use
- Consume excessive IT resources, (i.e.; Internet Bandwidth-streaming)

#### 1.2 Hardware:

- All computer hardware is the property of the County of Kaua'i and maintained by the Information Technology Division

Prepared by: Lynnette Meatoga	Date last revised: August 9, 2007	Page Number: 2/3
Original release date: August 9, 2007	Reviewed by : Eric Knutzen  Approved by: IT Steering Committee	

EXHIBIT C

  County of Kaua'i	<b>Information Technology Team</b>  <b>Standard Mobile Device Policy</b>	Documentation Number: ITP0025
		Revision Level: October 16, 2007

- Desktop systems and peripherals (printers, monitors, etc.) may only be moved by the Information Technology Division. The Department may call the Helpdesk to schedule moves

**1.3 Software Installation:**

- Only legal copies of County owned software can be loaded on computers. No individual users may load software. Information Technology Division must approve and load all software. Any software not approved and installed by I.T. will be removed (i.e., games, etc)
- No County owned software may be loaded on any non-County equipment (personal)
- 

- Users may not download software from the internet unless it is approved by I.T.
- Do not load any games on County owned Computers

**1.4 Saving files to computers and network drives**

- Do not store any mp3 files that is not related to work or the County's Mission
- Do not store any picture files (jpeg, etc.) that is not related to work or the County's Mission
- Do not store any video files that is not related to work or the County's Mission

**1. Access to Computers and Networking resources**


The County makes every effort to provide secure, reliable computing and networking resource. However, such measures are not foolproof and the security of a users electronic information is the responsibility of the user.

Under no circumstances may an external network be interconnected to act as a gateway to the County's network without coordination and approval from the I.T Division.

**1.1 Sharing of access**

Prepared by: Lynnette Meatoga	Date last revised: August 9, 2007	Page Number: 3/3
Original release date: August 9, 2007	Reviewed by : Eric Knutzen  Approved by: IT Steering Committee	

EXHIBIT C

  County of Kaua'i	<b>Information Technology Team</b>  <b>Standard Mobile Device Policy</b>	Documentation Number: ITP0025
		Revision Level: October 16, 2007

Access to computing and networking resources, computer accounts, password and other type of authorization are assigned to individual users must not be shared with others. Users are responsible for any use or misuse of their authentication information.

VI. **REFERENCE:** This document is to be updated by the Information Technology Team Manager, and is accessible by all County of Kaua'i employees at the IT Team Division.

Prepared by: Lynnette Meatoga	Date last revised: August 9, 2007	Page Number: 4/3
Original release date: August 9, 2007	Reviewed by : Eric Knutzen  Approved by: IT Steering Committee	



## County of Kaua'i

# Destruction of Records Policy

Documentation  
Number: ITP0029

Revision  
Level: 10/10/08

**I. SCOPE / PURPOSE:** The purpose of this policy is to describe how the County of Kaua'i (COK) coordinates its administration regarding the destruction of records, whether the records are in paper/hardcopy form or electronic form (hard disk, microfilm, or other electronic media).

EXHIBIT D

The scope of this policy regards the method by which all county related records may be destroyed. Such records include but are not limited to:

- ✓ Outdated records as defined by the County of Kauai Records Retention Schedule
- ✓ Records in hardcopy form (paper documents)
- ✓ Records in electronic form (email, CD, DVD, hard disk, video, audio, etc)
- ✓ Public or confidential information

**II. RESPONSIBILITY:** All agencies are responsible to follow the policy regarding records destruction as outlined here.

### III. DEFINITIONS:

"Records Destruction" = the act of permanently and concurrently destroying electronic or hard copy versions of any record or series of records.

"Records" = an item or collection of data retained by County of Kauai (paper or electronic media containing information pertaining to employees, transactions, or public information)

### IV. PROCEDURE:

- A. The department is to complete the attached Certificate of Destruction form, and save it electronically to the County of Kauai Laserfiche document repository in the "COK-IMAGING\County-wide\Certificates of Records Destruction" folder using the following file naming convention: DepartmentName YY-MM-DD
- B. When the shredding method is used, the shredder must cross-cut to no larger than 1/8"x1-1/8" pieces.
- C. To destroy electronic media, such as CD's or DVD's, the department may choose to send it to the IT Help Desk Clerk with Certificate of Destruction signed by the Department Head, describing the contents of the media. Upon destruction of the media, the certificate will also be signed by the IT Help Desk Clerk and a witness.
- D. The following people must sign the Certificate of Records Destruction form: the person destroying the records, a witness, and the Department Head.
- E. Questions regarding this policy may be forwarded to the IT Help Desk by calling 241-4400.

**V. REFERENCE:** This document is to be updated by the Information Technology Team Manager, and is accessible by all County of Kaua'i employees at the IT Team Division.

**VI. ATTACHMENTS:** Certificate of Records Destruction form. Electronic pdf versions are available on the Laserfiche document repository in the following folder:  
COK-IMAGING\County-wide\Certificates of Records Destruction.

Prepared by: Mandi Swanson	Date last revised: 10/10/08	Page Number: 1/2
Original release date: 9/30/08	Reviewed by : Eric Knutzen Approved by: Wallace Rezentes	





**COUNTY OF KAUAI  
PERSONAL INFORMATION SECURITY INCIDENT REPORT FORM**

<b>Reported by:</b>				<b>Today's Date:</b>			
<b>Phone:</b>				<b>Email:</b>			
<b>Division/Agency:</b>		<b>Incident or breach was discovered by:</b>		<b>Date Discovered:</b>		<b>Time Discovered:</b>	

<b>TYPE OF RECORDS:</b>	<b>MEDIA:</b>	<b>PERSONAL INFORMATION COMPROMISED:</b>

<b>SUSPECTED CAUSE OF INCIDENT/BREACH:</b>		
1.	Theft	
2.	Damaged or stolen equipment	
3.	Improper disposal/destruction	
4.	Computer Virus or Worm	
5.	Unauthorized/inappropriate use of software	
6.	Other	

<b>RECORD INFORMATION:</b>		
1.	Number of records	
2.	Location of records	
3.	Number of affected individuals	

<b>COK ACTIONS TAKEN SO FAR:</b>		
<b>Affected persons notified.</b>		
<b>System disconnected from network.</b>		
<b>System Back Up.</b>		
<b>Records retrieved.</b>		
<b>Security Breach Notice Prepared.</b>		
<b>Third party contractors notified.</b>		
<b>Law enforcement notified.</b>		

<b>SECURITY BREACH CRITERIA:</b>